

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2004-164287

(43)Date of publication of application : 10.06.2004

(51)Int.Cl. G06F 12/14
G09C 1/00
H04H 1/00
H04L 9/32
H04N 5/76
H04N 7/16

(21)Application number : 2002-329444

(71)Applicant : MATSUSHITA ELECTRIC IND CO
LTD

(22)Date of filing : 13.11.2002

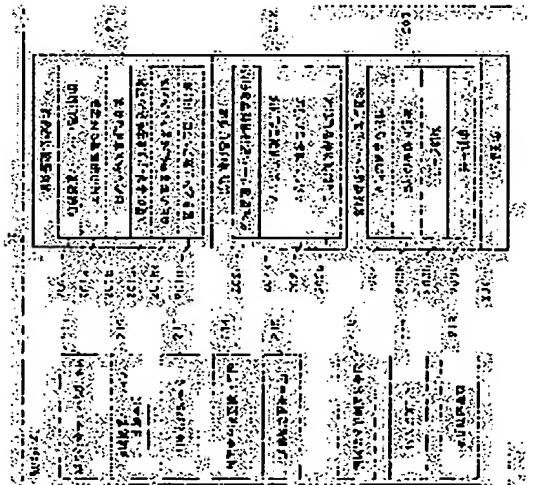
(72)Inventor : NIWANO SATOSHI
TOKUDA KATSUMI
MURAKAMI HIRONORI
INOUE MITSUHIRO
OMORI MOTOJI

(54) INFORMATION RECORDING SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a low-cost recording medium allowing safe recording of information without requiring consideration of a rewriting service life when using the recording medium.

SOLUTION: This recording medium 2 comprises: an area management server authentication means 211; an area configuration version comparison means 212; a user authentication means 213; a use command falsification detection means 214; an area configuration update means 215 changing an area configuration; an area configuration information requirement means 216 requiring area configuration information to an area management server 1; an individual authentication means 217 authenticating a holder of the recording medium 2; and a recording area and a recording medium identification 218 uniquely specifying the recording medium 2.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

BEST AVAILABLE COPY

(19) 日本国特許庁(JP)

(12) 公開特許公報(A)

(11) 特許出願公開番号

特開2004-164287

(P2004-164287A)

(43) 公開日 平成16年6月10日(2004.6.10)

(51) Int. Cl. ⁷

F 1

テーマコード (参考)

G06F 12/14
G09C 1/00
H04H 1/00
H04L 9/32
H04N 5/76

G06F 12/14 320C
G06F 12/14 310H
G09C 1/00 640D
H04H 1/00 F
H04N 5/76 Z

5B017
5C052
5C064
5J104

審査請求 未請求 請求項の数 27 O L (全 25 頁) 最終頁に続く

(21) 出願番号 特願2002-329444 (P2002-329444)
(22) 出願日 平成14年11月13日(2002.11.13)

(71) 出願人 000005821
松下電器産業株式会社
大阪府門真市大字門真1006番地
(74) 代理人 100097445
弁理士 岩橋 文雄
(74) 代理人 100103355
弁理士 坂口 智康
(74) 代理人 100109667
弁理士 内藤 浩樹
(72) 発明者 庭野 智
大阪府門真市大字門真1006番地 松下
電器産業株式会社内
(72) 発明者 徳田 克己
大阪府門真市大字門真1006番地 松下
電器産業株式会社内

最終頁に続く

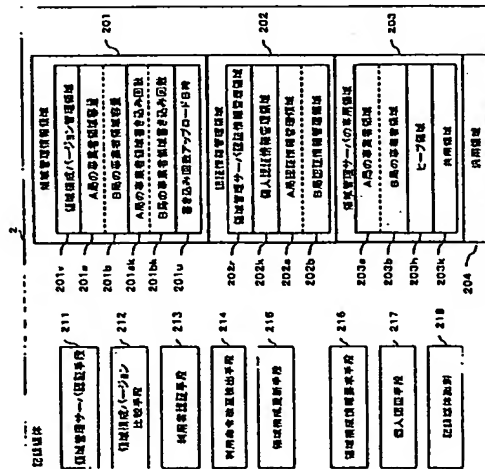
(54) 【発明の名称】 情報記録システム

(57) 【要約】

【課題】 利用に際して書き換え寿命を考慮する必要がなく、安全に情報の記録が可能で、安価に提供可能な記録媒体を提供する。

【解決手段】 記録媒体2は、領域管理サーバ認証手段211と、領域構成バージョン比較手段212と、利用者認証手段213と、利用命令改竄検出手段214と、領域構成を変更する領域構成更新手段215と、領域管理サーバ1に領域構成情報を要求する領域構成情報要求手段216と、記録媒体2の所有者の認証を行う個人認証手段217と、記録媒体2を一意に特定する記録媒体識別218と記録領域から構成される。

【選択図】 図3



【特許請求の範囲】

【請求項 1】

データ放送で記録媒体への情報の記録および読み込みを行う情報記録システムであって、
認証された利用者の利用命令により情報の記録および読み込みを行う領域を備えた記録媒体と、

前記記録媒体を着脱する受信機と、

前記記録媒体に利用命令と認証情報を配信する配信サーバと、

前記領域の領域構成を管理する領域管理サーバと

から構成されることを特徴とする情報記録システム。

【請求項 2】

前記記録媒体における前記認証された利用者の利用命令により情報の記録および読み込みを行う領域には、

第 1 の利用者の領域と、

前記第 1 の利用者の領域に第 2 の利用者の領域を備え、

前記第 1 および第 2 の利用者を認証する手段と、

前記第 1 および第 2 の利用者の利用命令の改竄を検出する手段と

を備えたことを特徴とする請求項 1 記載の情報記録システム。

【請求項 3】

前記第 1 の利用者が領域管理サーバであることを特徴とする請求項 2 記載の情報記録システム。

【請求項 4】

前記領域管理サーバはさらに、

前記記録媒体に第 1 の利用者の領域構成の変更を指示する手段を備えたことを特徴とする請求項 3 記載の情報記録システム。

【請求項 5】

前記第 1 の利用者の認証情報に前記第 1 の利用者の領域構成識別情報を含むことを特徴とする請求項 1 記載の情報記録システム。

【請求項 6】

前記領域管理サーバはさらに、

前記第 1 の利用者の領域構成識別情報を管理する手段を備えたことを特徴とする請求項 4 記載の情報記録システム。

【請求項 7】

前記記録媒体はさらに、

前記第 1 の利用者の領域構成識別情報を管理する手段を備えたことを特徴とする請求項 2 記載の情報記録システム。

【請求項 8】

前記記録媒体はさらに、

前記第 1 の利用者の領域構成識別情報の更新を識別する手段を備えたことを特徴とする請求項 7 記載の情報記録システム。

【請求項 9】

前記第 1 の利用者の領域を構成する情報を識別する情報が領域構成識別子であることを特徴とする請求項 5、請求項 6、または請求項 8 のいずれか 1 項に記載の情報記録システム。

【請求項 10】

前記第 1 の利用者の領域を構成する情報を識別する情報が前記第 2 の利用者の領域の容量であることを特徴とする請求項 5、請求項 6、請求項 8 のいずれか 1 項に記載の情報記録システム。

【請求項 11】

前記記録媒体はさらに、

個人認証情報を記録する領域と前記個人認証情報で個人認証する手段を備えたことを特徴

10

20

30

40

50

とする請求項 1 記載の情報記録システム。

【請求項 1 2】

前記領域管理サーバはさらに、

前記第 2 の利用者の領域の容量に比例した価値情報を前記第 2 の利用者に要求する手段を備えたことを特徴とする請求項 3 記載の情報記録システム。

【請求項 1 3】

前記領域管理サーバはさらに、

前記第 2 の利用者の領域の容量の変更回数に比例した価値情報を前記第 2 の利用者に要求する手段を備えたことを特徴とする請求項 3 記載の情報記録システム。

【請求項 1 4】

前記記録媒体はさらに、

前記第 2 の利用者の利用命令による書き込み回数を管理する手段を備えたことを特徴とする請求項 2 記載の情報記録システム。

【請求項 1 5】

前記領域管理サーバはさらに、

前記第 2 の利用者の領域への書き込み回数に比例した価値情報を前記第 2 の利用者に要求する手段を備えたことを特徴とする請求項 3 記載の情報記録システム。

【請求項 1 6】

前記記録媒体はさらに、

前記第 1 の利用者の領域に前記第 2 の利用者の情報を移動する領域を備えたことを特徴とする請求項 2 記載の情報記録システム。

【請求項 1 7】

前記記録媒体はさらに、

前記第 2 の利用者の情報を消去する規則を備えたことを特徴とする請求項 2 記載の情報記録システム。

【請求項 1 8】

前記領域管理サーバはさらに、

前記記録媒体の前記第 2 の利用者の情報を移動する領域を備えたことを特徴とする請求項 3 記載の情報記録システム。

【請求項 1 9】

前記記録媒体はさらに、

前記第 1 の利用者の領域に、少なくとも 1 つの第 2 の利用者が読み込みを行う共通領域を備えたことを特徴とする請求項 2 記載の情報記録システム。

【請求項 2 0】

前記記録媒体はさらに、

第 2 の利用者の認証情報で前記共通領域の読み込みを行うことを特徴とする請求項 1 9 記載の情報記録システム。

【請求項 2 1】

前記記録媒体はさらに、

前記記録媒体の所有者の承諾で前記共用領域の読み込みを行うことを特徴とする請求項 2 0 記載の情報記録システム。

【請求項 2 2】

前記記録媒体はさらに、

前記第 1 の利用者の領域に構成する第 2 の利用者を選択する手段を備えたこと請求項 2 記載の情報記録システム。

【請求項 2 3】

前記記録媒体はさらに、

前記第 1 の利用者の領域に構成した前記第 2 の利用者の領域に記録および読み込みを許可する第 2 の利用者を選択する手段と、

前記選択した利用者のリストを管理する手段と

10

20

30

40

50

を備えたことを特徴とする請求項2記載の情報記録システム。

【請求項24】

前記受信機はさらに、

前記第1の利用者の領域に構成した前記第2の利用者の領域に記録および読み込みを許可する第2の利用者を選択する手段と、

前記選択した利用者のリストを管理する手段と

を備えたことを特徴とする請求項1記載の情報記録システム。

【請求項25】

前記記録媒体はさらに、

前記第1の利用者の認証情報が記録されていることを特徴とする請求項2記載の情報記録システム。 10

【請求項26】

前記記録媒体はさらに、

前記第1の利用者の認証情報が変更可能なことを特徴とする請求項2記載の情報記録システム。

【請求項27】

利用命令を放送で配信することを特徴とする請求項1記載の情報記録システム。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、放送や通信などで、映像、音声などのデジタルコンテンツを配信し、ユーザが受信機でデジタルコンテンツを利用するシステムに関し、特に、受信機価格の書き換え寿命を考慮した利用自粛の必要がなく、情報の安全な一時記録を行う、情報記録システムおよび情報記録媒体に関する。 20

【0002】

【従来の技術】

従来のARIB (Association of Radio Industries and Businesses) 規格に準拠したデジタル放送受信機は、1次記憶装置 (RAM) と永続記憶装置 (NVRAM) が実装されている。

【0003】

1次記憶装置は、データ放送で配信されるXML (Extensible Markup Language) をベースにしたマルチメディア符号化方式BML (Broadcasting Markup Language) で作成されたコンテンツをBMLブラウザが読み込んで画面に表示するために、カールセル化され配信されたBMLを一時的に記録しておくために用いられ、永続記憶装置は、BMLの放送用拡張関数により、例えば地域情報やゲームのスコアなどの情報を記録、読み込むために用いられる (例えば、特許文献1参照。)。また、受信機内に実装された永続記憶装置の代わりに、受信機外のカードを利用しているものもある (例えば、特許文献2参照)。 30

【0004】

【特許文献1】

特開2001-320341号公報 40

【特許文献2】

特表平9-508993号公報

【0005】

【発明が解決しようとする課題】

永続記憶装置に用いられる不揮発性メモリは書き換え寿命があり、書き込みを頻繁に行うと受信機の寿命が短くなるため、ARIB規格において、運用のガイドラインが策定されるなど、利用には制限が必要だった。また、永続記憶装置の中の情報を保護するための仕組みがないため、秘匿性の高いプライバシー情報やポイント情報などの価値の高い情報を記録する運用は控えられている。 50

【0006】

受信機に実装された永続記憶装置には以上のような課題があるが、受信機価格を低廉にするため、永続記憶装置の機能拡張は行われていない。また、受信機外のカードなどの記録媒体を利用する場合、記録媒体への書き込み頻度、書き込み容量などは、記録媒体を利用する放送局毎に異なるため、記録媒体のコスト分配をどのように行うかは問題であった。

【0007】

本発明は、こうした従来の問題点を解決するものであり、受信機から着脱可能で情報の安全な記録が可能な記録媒体を永続記憶装置として用いることにより、書き換え寿命が来ても取り外しが可能なため交換できるため、放送局が、書き換え寿命を考慮して利用を自主規制する必要がなく、所有者のプライバシー情報やポイント情報などを安全に記録することが可能で、放送局の利用状況に応じた記録媒体のコスト分配を行う記録媒体と情報記録システムを提供することを目的としている。

【0008】

【課題を解決するための手段】

上記目的を達成するために、本発明では、データ放送で記録媒体への情報の記録および読み込みを行う情報記録システムであって、認証された利用者の利用命令により情報の記録および読み込みを行う領域を備えた記録媒体と、前記記録媒体を着脱する受信機と、前記記録媒体に利用命令と認証情報を配信する配信サーバと、前記領域の領域構成を管理する領域管理サーバとから構成されることを特徴とする情報記録システムを提供する。

【0009】

また、本発明では、前記認証された利用者の利用命令により情報の記録および読み込みを行う領域には第1の利用者の領域と、前記第1の利用者の領域に第2の利用者の領域を備え、前記第1および第2の利用者を認証する手段と、前記第1および第2の利用者の利用命令の改竄を検出する手段を備えたことを特徴とする記録媒体を提供する。

【0010】

また、本発明では、前記第1の利用者が領域管理サーバであることを特徴とする情報記録システムを提供する。

【0011】

また、本発明では、前記記録媒体に第1の利用者の領域構成の変更を指示する手段を備えたことを特徴とする領域管理サーバを提供する。

【0012】

また、本発明では、前記第1の利用者の認証情報に前記第1の利用者の領域構成識別情報を含むことを特徴とする情報記録システムを提供する。

【0013】

また、本発明では、前記第1の利用者の領域構成識別情報を管理する手段を備えたことを特徴とする領域管理サーバを提供する。

【0014】

また、本発明では、前記第1の利用者の領域構成識別情報を管理する手段を備えたことを特徴とする記録媒体を提供する。

【0015】

また、本発明では、前記第1の利用者の領域構成識別情報の更新を識別する手段を備えたことを特徴とする記録媒体を提供する。

【0016】

また、本発明では、前記第1の利用者の領域を構成する情報を識別する情報が領域構成識別子であることを特徴とする情報記録システムを提供する。

【0017】

また、本発明では、前記第1の利用者の領域を構成する情報を識別する情報が前記第2の利用者の領域の容量であることを特徴とする情報記録システムを提供する。

【0018】

また、本発明では、個人認証情報を記録する領域と前記個人認証情報で個人認証する手段

10

20

30

40

50

を備えたことを特徴とする記録媒体を提供する。

【0019】

また、本発明では、前記第2の利用者の領域の容量に比例した価値情報を前記第2の利用者に要求する手段を備えたことを特徴とする領域管理サーバを提供する。

【0020】

また、本発明では、前記第2の利用者の領域の容量の変更回数に比例した価値情報を前記第2の利用者に要求する手段を備えたことを特徴とする領域管理サーバを提供する。

【0021】

また、本発明では、前記第2の利用者の利用命令による書き込み回数を管理する手段を備えたことを特徴とする記録媒体を提供する。

10

【0022】

また、本発明では、前記第2の利用者の領域への書き込み回数に比例した価値情報を前記第2の利用者に要求する手段を備えたことを特徴とする領域管理サーバを提供する。

【0023】

また、本発明では、前記第1の利用者の領域に前記第2の利用者の情報を移動する領域を備えたことを特徴とする記録媒体を提供する。

【0024】

また、本発明では、前記第2の利用者の情報を消去する規則を備えたことを特徴とする記録媒体を提供する。

【0025】

また、本発明では、前記記録媒体の前記第2の利用者の情報を移動する領域を備えたことを特徴とする領域管理サーバを提供する。

20

【0026】

また、本発明では、前記第1の利用者の領域に、少なくとも1つの第2の利用者が読み込みを行う共通領域を備えたことを特徴とする記録媒体を提供する。

【0027】

また、本発明では、第2の利用者の認証情報で前記共通領域の読み込みを行うことを特徴とする記録媒体を提供する。

【0028】

また、本発明では、前記記録媒体の所有者の承諾で前記共用領域の読み込みを行うことを特徴とする記録媒体を提供する。

30

【0029】

また、本発明では、前記第1の利用者の領域に構成する第2の利用者を選択する手段を備えたこと記録媒体を提供する。

【0030】

また、本発明では、前記第1の利用者の領域に構成した前記第2の利用者の領域に記録および読み込みを許可する第2の利用者を選択する手段と、前記選択した利用者のリストを管理する手段を備えたこと記録媒体を提供する。

【0031】

また、本発明では、前記第1の利用者の領域に構成した前記第2の利用者の領域に記録および読み込みを許可する第2の利用者を選択する手段と、前記選択した利用者のリストを管理する手段を備えたことを特徴とする受信機を提供する。

40

【0032】

また、本発明では、前記第1の利用者の認証情報が記録されていることを特徴とする記録媒体を提供する。

【0033】

また、本発明では、前記第1の利用者の認証情報が変更可能なことを特徴とする記録媒体を提供する。

【0034】

また、本発明では、利用命令を放送で配信することを特徴とする情報記録システムを提供

50

する。

【0035】

【発明の実施の形態】

以下、本発明の実施の形態について、図面を用いて詳細に説明する。

【0036】

図1は、本発明の実施の形態に関わる情報記録システムの全体の概略構成を示す図である。

【0037】

この情報記録システムは、通信販売の購入履歴、または、クイズに答えて獲得したポイントなどを、サービスを行う事業者に割り当てた領域に安全に記録し、また、事業者のサービス規模が変化した場合に領域の容量の変更を可能とするために、領域管理サーバの専用領域の中に放送局の事業者領域を含む記録媒体2に、ネットワークを通じて放送局4から配信される利用命令を用いて情報の安全な記録と読み出しと、事業者領域の更新を行うシステムであり、利用命令を配信する配信サーバ5と、利用命令を受信する受信機3と、受信機3から着脱可能な記録媒体2と、記録媒体2の領域構成を管理する領域管理サーバ1と記録媒体2の事業者領域を利用する放送局4とから構成される。

【0038】

ネットワークに接続された領域管理サーバ1と、受信機3と、放送局4と、配信サーバ5はそれぞれ、ネットワークからデータを送受信する手段（図1には示さない）を備えている。

【0039】

ここで、ネットワークとは、放送および通信のことを指し、例えば、放送で配信サーバ5から受信機3への利用命令の配信する場合は、データ放送により利用命令を含んだBMLスクリプトをBMLコンテンツとしてカルーセル化して配信する方法がある。ただし、カルーセル化されたBMLコンテンツ以外の方法、および、通信による方法であっても、利用命令が受信機3に配信されればよい。

【0040】

また、利用命令とは、受信機3または受信機3に接続された各種資源の利用および制御を行うものであり、例えば、BMLの放送用拡張関数があるが、これに限らず同様な機能を持つものであればよい。

【0041】

図2は、本発明の実施の形態に関わる領域管理サーバ1の概略構成を示す機能ブロック図である。

【0042】

図2に示すように、領域管理サーバ1は、領域構成情報管理手段101と、領域構成変更指示手段102と、認証情報付加手段103と、書き込み回数管理手段104と、記録媒体数管理手段105と、利用コスト算出手段106と、認証情報付加回数管理手段107とから構成される。以下、それぞれの構成要素について説明する。

【0043】

領域構成情報管理手段101は、記録媒体2の領域を構成する情報を格納するデータベースを管理しており、当該データベースは図7に例示するように、記録媒体2ごとに、領域構成バージョンのバージョン番号、事業者、事業者領域容量、容量変更回数、認証情報などを格納している。

【0044】

領域構成バージョンのバージョン番号とは、記録媒体2の領域を構成するバージョン番号であり、図7の例では“1.1”が記述されている。事業者とは記録媒体2を用いて各種サービスを行う事業者を表し、図7の例では、“A局”、“B局”の2つが記述されている。事業者領域容量とは、記録媒体2を用いて各種サービスを行う事業者ごとに割り当てられたメモリ容量のことであり、図7の例では、事業者A局に対して“5MB”、事業者B局に対して“2MB”が割り当てられていることを示している。また、容量変更回数と

は、各事業者が記録媒体2の容量を変更した回数を示す情報であり、図7の例では、事業者A局が“1回”、事業者B局が“2回”、それぞれ容量を変更したことを示している。認証情報とは、放送局4から登録された秘密鍵と署名から成る情報であり、図7の例では事業者A局に対する認証情報が“0 x F F F F”、事業者B局に対する認証情報が“0 x A F F F”と記述されている。

【0045】

領域構成変更指示手段102は、領域構成バージョン更新時および記録媒体2からの要求時に領域構成情報を配信する。また、認証情報付加手段103は、証明書を領域管理サーバ1の秘密鍵で暗号化する処理を行う。

【0046】

書き込み回数管理手段104は、全記録媒体2から受信した記録媒体2の事業者領域の書き込み回数を格納するデータベースを管理しており、当該データベースは受信した記録媒体2の事業者領域の書き込み回数合計として例えば“10000回”などの回数を格納している。

【0047】

記録媒体数管理手段105は、受信機3を通じて記録媒体2から受信した記録媒体2の登録数を格納するデータベースを管理しており、当該データベースは登録数として“1000枚”などの登録数を格納している。

【0048】

利用コスト算出手段106は、記録媒体2に事業者領域を構成している放送局4に対して記録媒体2の月額利用料金を算出する手段であり、月額利用料金とは、例えば、記録媒体数管理手段105で管理されている記録媒体2の登録出荷枚数に対して、(1)領域構成情報管理手段101で管理している利用事業者領域容量1MB毎に10円として加算、(2)1ヶ月の容量変更1回毎に100円として加算する。また、(3)認証情報付加回数管理手段107で管理されている1ヶ月の認証情報付加1回毎に20円として加算する。また、書き込み回数管理手段104で管理している全記録媒体2に対して(4)1ヶ月の書き込み1回毎に30円として加算する。なお利用コストの算出に際しては、上記(1)～(4)をすべて用いて算出してもよいし、上記(1)～(4)のいずれかのみ用いて算出してもよい。

【0049】

認証情報付加回数管理手段107は、認証情報付加手段103で証明書を発行した回数を格納するデータベースを管理しており、当該データベースは例えば証明書を発行した回数として“30回”などの発行回数を格納している。

【0050】

図3は、本発明の実施の形態に関わる記録媒体2の概略構成を示す図である。

【0051】

記録媒体2はコントローラとフラッシュメモリから構成される半導体メモリカードであり、コントローラで認証された利用命令にしたがってフラッシュメモリに情報を記録する。

【0052】

記録媒体2には、領域管理サーバ1の証明書を確認する領域管理サーバ認証手段211と、配信された利用命令に含まれる領域構成バージョンと領域構成バージョン管理領域201に記録された領域構成バージョンとを比較する領域構成バージョン比較手段212と、配信された放送局4の証明書を局の認証情報を用いて確認する利用者認証手段213と、配信されたスクリプトのハッシュ計算し、証明書に含まれるハッシュ値と比較する利用命令改竄検出手段214と、領域管理サーバ1からの指示で領域構成を変更する領域構成更新手段215と、領域構成が最新でない場合に領域管理サーバ1に領域構成情報を要求する領域構成情報要求手段216と、記録媒体2の所有者の認証を行う個人認証手段217と、記録媒体2を一意に特定する記録媒体識別218と記録領域から構成される。

【0053】

図16は、本発明の実施の形態に関わる記録媒体2の記録領域の一般的なデータ構造を示

10

20

30

40

50

す図である。

【0054】

記録媒体2の記録領域は、記録されるデータの種類から、領域管理情報領域1601と、認証情報管理領域1602と、領域管理サーバの専用領域1603と、汎用領域1604とに分けられる。

【0055】

領域管理情報領域1601は、領域管理に関するデータの記録に用いられ、データ領域として、領域構成バージョン管理領域1601vと、事業者領域容量1601aと、事業者領域書き込み回数1601akと、書き込み回数アップロード日時1601uとから構成される。なお、事業者領域容量1601aと、事業者領域書き込み回数1601akは記録媒体2の利用者毎に領域が分割される。

10

【0056】

認証情報管理領域1602は、記録媒体2の利用者の認証に関するデータの記録に用いられ、領域管理サーバ認証情報管理領域1602rと、個人認証情報管理領域1602kと、事業者認証情報管理領域1602aとから構成される。なお、事業者認証情報管理領域1602aは記録媒体2の利用者毎に領域が分割される。

【0057】

領域管理サーバの専用領域1603は、記録媒体2の利用者と所有者によるデータの記録に用いられ、事業者領域1603aと、ヒープ領域1603hと、共用領域1603kとから構成される。なお、事業者領域1603aは記録媒体2の利用者毎に領域が分割される。

20

【0058】

次に図3を用いて、A局とB局が領域管理サーバ1に利用登録している場合の記録領域の構成について説明する。

【0059】

記録領域の領域管理情報領域201には、領域構成情報に基づいて、領域構成のバージョンが領域構成バージョン管理領域201vに、A局の利用可能な容量がA局の事業者領域容量201aに、B局の利用可能な容量がB局の事業者領域容量201bに、A局の事業者領域書き込み回数がA局の事業者領域書き込み回数201akに、B局の事業者領域書き込み回数がB局の事業者領域書き込み回数201bkに、事業者領域書き込み回数を領域管理サーバ1へアップロードする日時が書き込み回数アップロード日時201uに記録される。

30

【0060】

また、記録領域の認証情報管理領域202には、例えばパスワードが個人認証情報管理領域202kに記録される。また、例えば秘密鍵および署名といった認証情報が、領域管理サーバ認証情報管理領域202rと、A局認証情報管理領域202aと、B局認証情報管理領域202bに記録される。

【0061】

領域管理サーバの専用領域203には、A局の事業者領域203aと、B局の事業者領域203bと、領域構成変更時にA局の事業者領域203aと、B局の事業者領域203bの情報が一時退避されるヒープ領域203hと、記録媒体2の所有者の個人データなどが記録される。また、図16で説明したように、領域管理サーバの専用領域203には、事業者領域を持つ放送局4が読むことが可能な共用領域203kを備える。

40

【0062】

さらに、記録媒体2は、所有者が自由に利用可能な汎用領域204を備える。

【0063】

図4は、本発明の実施の形態に関わる放送局4の概略構成を示す図である。

【0064】

放送局4は、利用命令を含むBMLスクリプトを作成するデータ放送制作手段401と、BMLスクリプトのハッシュ値を含む証明書を作成し、放送局4の秘密鍵で暗号化する認

50

証情報作成手段402と、認証情報作成手段402で作成した証明書に領域管理サーバ1の証明書の付加を要求する認証情報要求手段403と、領域管理サーバ1に事業者領域の容量変更を指示する容量変更指示手段404と、領域管理サーバ1に記録媒体2の利用料を支払う決済処理を行う利用料支払手段405とから構成される。

【0065】

このような情報記録システムにおいて、データ放送を利用した通信販売を例に、図5から図15、図17、図18の図面を用いて説明する。

【0066】

(記録媒体2の初期化)

記録媒体2の所有者は、記録媒体2の事業者領域を利用している放送局がコストの一部を負担することで、同じ容量の他の記録媒体よりも安い価格で販売されている記録媒体2を購入する。なお、記録媒体2が受信機3に同梱されている場合、同梱されている記録媒体2を利用してもよい。

【0067】

購入直後の記録媒体2の記録領域の状態を図5に示す。

【0068】

購入直後は、領域管理情報領域201には、領域構成バージョン管理領域201vがあるだけで、他のデータは記録されていない。領域構成バージョン管理領域201vには、例えば、“0.0”と記録されている。

【0069】

また、認証情報管理領域202には、領域管理サーバ認証情報管理領域202rがあるだけで、他のデータは記録されていない。領域管理サーバ認証情報管理領域202rには、領域管理サーバ1の秘密鍵が記録されている。

【0070】

また、領域管理サーバの専用領域203には、ヒープ領域203hと共用領域203kが構成されているだけで、事業者の領域は構成されていない。

【0071】

また、汎用領域204には何も記録されていない。

【0072】

次に、図8のフローチャートを用いて記録媒体2の初期化の動作について説明する。

【0073】

所有者が記録媒体2を受信機3に挿入すると(S101)、受信機3から記録媒体2へ起動命令が送信され、記録媒体2では起動処理が開始される(S102)。

【0074】

記録媒体2の起動処理では、領域構成バージョン比較手段212で領域構成バージョン管理領域201vから領域構成バージョンを取得する(S103)。取得した領域構成バージョンが“1.0”のような領域構成後の値であれば(S104でYES)領域構成済みであると判断し、受信機3に起動終了を通知する(S117)。一方、取得した領域構成バージョンが“0.0”のような購入直後の値である場合(S104でNO)、領域構成が必要であると判断し、受信機3に領域構成要求を通知する(S105)。

【0075】

受信機3は記録媒体2に領域構成指示を送信する(S106)。

【0076】

記録媒体2は、領域構成情報要求手段216により、受信機3に記録媒体識別218を送信すると共に領域構成情報を要求し(S107)、この要求を受けた受信機3は、領域管理サーバ1へ記録媒体識別218を送信すると共に領域構成情報を要求する(S108)。

【0077】

領域管理サーバ1は記録媒体2からの記録媒体識別218と領域構成情報要求を受信すると、記録媒体数管理手段105に記録媒体識別218を記録し、記録媒体数管理手段10

10

20

30

40

50

5では記録媒体識別218の総数を記録媒体2の登録数として共に管理する。

【0078】

次に、領域構成変更指示手段102が領域構成情報管理手段101から領域構成バージョンと、事前にA局とB局から登録されていたA局の事業者領域容量と、B局の事業者領域容量と、A局認証情報と、B局認証情報とを取得し、領域管理サーバ1が設定した、例えば“2002年10月23日”のような、書き込み回数アップロード日時と、領域更新するための利用命令、例えばX-flash-quotaPersistent()と、記録媒体2の所有者の個人情報を用いて領域に記録するための利用命令、例えばX-flash-writePersistentString()とを含んだBMLスクリプトと共に認証情報付加手段103に送信する(S109)。

10

【0079】

認証情報付加手段103は、認証情報付加回数管理手段107の証明書を発行回数を1加算し、書き込み回数アップロード日時と利用命令を含んだBMLスクリプトから計算したスクリプトのハッシュ601と、領域構成バージョン602と、A局の事業者領域容量603と、B局の事業者領域容量604と、“0xFFFF”などの秘密鍵と署名から成るA局認証情報605と、B局認証情報606と、領域管理サーバの署名607とを図6に示すように領域管理サーバ1の証明書600に格納して、領域管理サーバ1の秘密鍵で暗号化して領域構成変更指示手段102に送信する(S110)。

【0080】

領域構成変更指示手段102は、BMLスクリプトと証明書を受信機3に送信し、受信機3は記録媒体2にBMLスクリプトと証明書を送信する(S111)。

20

【0081】

記録媒体2は、受信したBMLスクリプトと証明書を領域管理サーバ認証手段211に送信する。

【0082】

領域管理サーバ認証手段211は、BMLスクリプトのハッシュ値を計算し、領域管理サーバ認証情報管理領域202rから取得した領域管理サーバ1の秘密鍵で証明書を復号し、領域管理サーバの署名607を確認し、計算したBMLスクリプトのハッシュ値と証明書に格納されていたスクリプトのハッシュ値601を比較し(S112)、一致していれば、領域構成バージョン602とA局の事業者領域容量603とB局の事業者領域容量604とA局認証情報605とB局認証情報606とを領域構成更新手段215に送信する。一致していなければ、改竄されていると判断して受信機に異常終了通知し(S118)、受信機3は異常終了画面を表示する(S119)。

30

【0083】

領域構成更新手段215は、領域構成バージョン602とA局の事業者領域容量603とB局の事業者領域容量604とから領域管理情報領域201を設定し、A局認証情報605とB局認証情報606とから認証情報管理領域202を設定し、A局の事業者領域容量603とB局の事業者領域容量604とから領域管理サーバの専用領域203を設定し、書き込み回数アップロード日時を書き込み回数アップロード日時201uに記録して領域構成が終了したことを受信機3に通知する(S113)。

40

【0084】

受信機3は個人情報入力画面を表示し、記録媒体2の所有者が入力した氏名、住所、クレジットカード番号などの個人情報と、パスワードなどの個人認証情報を記録媒体2に送信する(S114)。

【0085】

記録媒体2は、個人情報を共用領域203kに、個人認証情報を個人認証情報管理領域202kに、例えばXML形式で記録し(S116)、起動終了を受信機3に通知し(S117)、受信機は記録媒体2の起動完了を認識する(S119)。

【0086】

なお、記録媒体2の初期化後は、記録媒体2を受信機3に挿入して個人認証終了後に記録

50

媒体 2 の領域管理サーバの専用領域 203 の利用が可能になる。

【0087】

なお、本実施の形態では、あらかじめ記録媒体 2 に領域管理サーバの専用領域 203 が記録されて販売されていたが、初期化時に領域管理サーバの専用領域 203 が構成されてもよい。

【0088】

なお、本実施の形態では、領域管理サーバ 1 に登録されている全ての放送局 4 の事業者領域を構成したが、領域構成する放送局 4 を記録媒体 2 の所有者が選択できてもよい。

【0089】

なお、本実施の形態では、領域管理サーバ 1 に登録されている全ての放送局 4 の事業者領域を構成したが、記録媒体 2 の所有者が選択した放送局 4 のリストを記録媒体 2 または受信機 3 に記録し、リストにより利用を制限してもよい。

【0090】

(記録媒体 2 の領域構成の変更)

次に、図 10 のフローチャートを用いて、記録媒体 2 の領域構成の変更を行う動作について説明する。なお、本実施の形態では、当該サービスを利用するすべての記録媒体 2 を対象に領域構成の変更処理を行うものとする。

【0091】

放送局 4 は、ここでは例えば A 局とする、容量変更指示手段 404 から、記録媒体 2 における A 局の事業者領域 203 a の容量の変更要求を領域管理サーバ 1 に送信する (S201)。

【0092】

領域管理サーバ 1 は A 局の事業者領域容量の変更要求を受信すると、領域構成変更指示手段 102 が、領域更新するための利用命令、例えば `X-flash-quotaPersistent()`、を含んだ BML スクリプトを作成し、領域構成情報管理手段 101 に A 局の事業者領域容量の変更を指示する (S202)。

【0093】

領域構成情報管理手段 101 では、例えば図 7 に示すようなテーブルを管理しており、A 局の事業者領域容量のデータを A 局から要求された容量に変更して、A 局の容量変更回数を 1 増加して、領域構成バージョンを、例えば、“1.0” から “1.1” に変更する (S203)。

【0094】

領域管理サーバ 1 は、領域構成情報管理手段 101 から領域構成バージョンと A 局の事業者領域容量と B 局の事業者領域容量と A 局認証情報と B 局認証情報とを取得し、領域更新するための利用命令を含んだ BML スクリプトと共に認証情報付加手段 103 に送信する。

【0095】

認証情報付加手段 103 は、認証情報付加回数管理手段 107 の証明書を発行回数を 1 加算し、BML スクリプトから計算したスクリプトのハッシュ 601 と、領域構成バージョン 602 と A 局の事業者領域容量 603 と B 局の事業者領域容量 604 と A 局認証情報 605 と B 局認証情報 606 とを図 6 に示す領域管理サーバの証明書 600 に格納して、領域管理サーバ 1 の秘密鍵で暗号化して領域構成変更指示手段 102 に送信する (S204)。

【0096】

領域構成変更指示手段 102 は、多くのチャンネルで領域変更するための利用命令を配信し、全記録媒体一斉の領域更新を速やかに実行するために、BML スクリプトと領域管理サーバ 1 の証明書を A 局と B 局に送信する。

【0097】

A 局と B 局は BML スクリプトと領域管理サーバ 1 の証明書から BML コンテンツを作成 (S205) し、配信サーバ 5 に送信する (S206)。

10

20

30

40

50

【0098】

配信サーバ5は、BMLスクリプトと領域管理サーバ1の証明書を含んだBMLコンテンツを受信(S207)し、データ放送で配信する(S208)。

【0099】

受信機3は記録媒体2の領域更新するための利用命令を含むBMLスクリプトと領域管理サーバ1の秘密鍵で暗号化された証明書が含まれているBMLコンテンツをデータ放送で受信し、領域更新するための利用命令に従い、BMLコンテンツを記録媒体2に送信する(S209)。

【0100】

記録媒体2では、領域管理サーバ認証手段211が、領域管理サーバ認証情報管理領域202rから領域管理サーバの秘密鍵を取り出し、領域管理サーバ1の証明書を復号し、領域管理サーバの署名を確認し、確認できた場合は、BMLコンテンツを利用命令改竄検出手段214に送信する(S210)。 10

【0101】

利用命令改竄検出手段214では、BMLスクリプトのハッシュ値を計算し、領域管理サーバ1の証明書に含まれているBMLスクリプトのハッシュ値と比較して(S211)、一致していれば、領域管理サーバ1の証明書に含まれている領域構成バージョンを領域構成バージョン比較手段212に送信し、不一致の場合、改竄されていると判断して処理を終了する(S214)。

【0102】

領域構成バージョン比較手段212では、領域構成バージョン管理領域201vから領域構成バージョンを取得し、領域管理サーバ1の証明書に記述されている領域構成バージョンと比較し、領域構成が更新されていることを確認し、領域管理サーバ1の証明書を領域構成更新手段215に送信する(S212)。 20

【0103】

領域構成更新手段215は、A局の事業者領域203aとB局の事業者領域203bの情報をヒープ領域203hに移動し、領域管理サーバ1の証明書から領域構成バージョンとA局の事業者領域容量とB局の事業者領域容量とを取得し、領域管理情報領域201に設定し、領域管理サーバの専用領域203にA局の事業者領域203aとB局の事業者領域203bを構成し、A局認証情報とB局認証情報とを取得し、認証情報管理領域202に設定し、ヒープ領域203hから情報をA局の事業者領域203aとB局の事業者領域203bに戻す(S213)。 30

【0104】

なお、事業者領域に記録されている情報に記録時のタイムスタンプも記録されており、領域構成更新により事業者領域が縮小し情報があふれてしまう場合には、例えば古い情報から削除するなどのルールに基づいて処理を行う図には示さない判定手段があってもよい。

【0105】

なお、領域管理サーバ1に図には示さない事業者領域の一時退避領域がある場合には、領域構成更新前に領域構成更新手段215が、事業者領域の情報を領域管理サーバ1にアップロードし、領域構成更新後にダウンロードしてもよい。この場合、領域管理サーバ1と記録媒体2とは、例えばSSLのような安全な通信路を確保して通信する。 40

【0106】

なお、本実施の形態では、領域管理サーバ1において領域構成更新するための利用命令を含んだBMLスクリプトを作成したが、記録媒体2の領域構成バージョン比較手段212で、領域構成バージョンが更新されていると判断される場合には、領域構成更新するための利用命令を受信せずに領域構成を更新してもよい。

【0107】

(通信販売を行うBMLスクリプトの作成)

次に、図11、図12、図13のフローチャートを用いて、通信販売を行う際の動作について説明する。 50

【0108】

放送局4は(ここでは例えばA局とする)、データ放送で通信販売を行うために、記録媒体2の領域管理サーバの専用領域203から情報を読み出す利用命令、例えばX-flash-readPersistentString()、を含む通信販売のBMLスクリプトを作成し(S301)、利用者であるA局の利用者の署名610と、BMLスクリプトのハッシュ601とを含む利用者の証明書609を作成し、A局の秘密鍵で暗号化する(S302)。

【0109】

作成したBMLスクリプトでは、利用命令でA局の事業者領域203aから読み出した購入履歴をBMLブラウザで表示する。また、記録媒体2の所有者がBMLブラウザにより表示される購入画面上で商品を購入すると、利用命令で読み出した記録媒体2の所有者の住所、氏名、クレジットカード番号などの個人情報を、記録媒体2の所有者が購入した商品番号と共にA局に送信する。

【0110】

A局は利用者の証明書609を領域管理サーバ1に送信する。

【0111】

領域管理サーバ1は、認証情報付加回数管理手段107の証明書を発行回数を1加算し、図9に示すように、領域構成バージョン602と、A局の事業者領域容量603と、B局の事業者領域容量604と、A局認証情報605と、B局認証情報606と、領域管理サーバの署名607と、A局を示す利用者識別608と、A局から受信した利用者の証明書609とを含む領域管理サーバの証明書600を作成し、領域管理サーバ1の秘密鍵で暗号化(S303)して、放送局4に送信する(S304)。

【0112】

放送局4は、領域管理サーバ1の利用者の証明書609とBMLスクリプトとを含むBMLコンテンツを作成し、配信サーバ5に送信する(S305)。

【0113】

配信サーバ5は、BMLコンテンツを受信(S306)し、データ放送で配信する(S307)。

【0114】

(記録媒体の利用)

受信機3はBMLコンテンツをデータ放送で受信し、BMLスクリプトに従い、BMLスクリプトと証明書が記録媒体2に送信される。

【0115】

記録媒体2では、領域管理サーバ認証手段211が、領域管理サーバ認証情報管理領域202rから領域管理サーバの秘密鍵を取り出し、領域管理サーバ1の証明書を復号し、領域管理サーバ1の署名を確認し、確認できた場合は、領域構成バージョン比較手段212に送信する(S308)。

【0116】

領域構成バージョン比較手段212では、領域構成バージョン管理領域201vから領域構成バージョンを取得し、領域管理サーバ1の証明書に記述されている領域構成バージョンと比較し(S309)、一致している場合、証明書を利用者認証手段213に送信し、不一致の場合、領域構成が必要であると判断し、受信機3に領域構成要求を通知し(S340)、図8のS106以降の処理を行う。

【0117】

利用者認証手段213では、利用者識別608から利用者がA局であることを認識し、A局認証情報管理領域202aからA局の秘密鍵を取り出し、利用者の証明書609を復号し、利用者の署名610がA局であることを確認し(S310)、確認できた場合は、BMLスクリプトと証明書を利用命令改竄検出手段214に送信する。一方、確認できなかった場合は異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

10

20

30

40

50

【0118】

利用命令改竄検出手段214では、BMLスクリプトのハッシュ601を計算し、領域管理サーバ1の証明書に含まれているBMLスクリプトのハッシュ601と比較して(S311)、一致している場合は、利用命令に従って、A局の事業者領域203aから購入履歴を読みだして受信機3に送信し(S312)、不一致の場合は異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0119】

受信機3では、BMLスクリプトと記録媒体2のA局の事業者領域203aから読み出した購入履歴から通信販売の購入画面をBMLブラウザで表示する(S313)。

【0120】

例えば、家庭用電気製品の通信販売のBMLスクリプトで、記録媒体2から読み出した購入履歴が“冷蔵庫”であったとすると、図14に示す購入画面が表示される。

【0121】

記録媒体2の所有者がBMLブラウザの表示する画面上の購入ボタンを押すと、利用命令によりBMLスクリプトと証明書が記録媒体2に送信され(S314)、記録媒体2では、領域管理サーバ認証手段211が、領域管理サーバ認証情報管理領域202rから領域管理サーバ1の秘密鍵を取り出し、領域管理サーバ1の証明書を復号し、領域管理サーバ1の署名を確認し、確認できた場合は、領域構成バージョンを領域構成バージョン比較手段212に送信し(S315)、確認できなかった場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0122】

領域構成バージョン比較手段212では、領域構成バージョン管理手段201vから領域構成バージョンを取得し、領域管理サーバ1の証明書に記述されている領域構成バージョンと比較し、一致している場合は、証明書を利用者認証手段213に送信し(S316)、不一致の場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0123】

利用者認証手段213では、利用者識別608から利用者がA局であることを認識し、A局認証情報管理領域202aからA局の秘密鍵を取り出し、A局の証明書を復号し、A局の署名を確認し、確認できた場合は、BMLスクリプトと証明書を利用命令改竄検出手段214に送信し(S317)、確認できなかった場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0124】

利用命令改竄検出手段214では、BMLスクリプトのハッシュ601を計算し、領域管理サーバ1の証明書に含まれているBMLスクリプトのハッシュ601と比較し(S318)、一致している場合は、利用命令に従って、記録媒体2の所有者の個人情報を共用領域203kから読みだしてA局に送信し(S319)、不一致の場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0125】

なお、本実施の形態では、領域管理サーバの専用領域203の利用者の証明書609で共用領域203kの利用を許可しているが、利用前にアラートを出して、ユーザの承諾により利用を許可してもよい。

【0126】

(放送局での課金処理と記録媒体への購入履歴記録)

A局では、記録媒体2の所有者の個人情報で課金処理を行い(S320)、記録媒体2のA局の事業者領域203aに購入した商品の購入履歴を記録する利用命令、例えばX-f l a s h - w r i t e P e r s i s t e n t S t r i n g ()、を含む課金完了のBMLスクリプトを作成し(S321)、利用者であるA局の利用者の署名610と、BMLスクリプトのハッシュ601とを含む利用者の証明書609を作成し、A局の秘密鍵で暗号化する(S322)。

10

20

30

40

50

【0127】

A局は両者の証明書609を領域管理サーバ1に送信する。

【0128】

領域管理サーバ1は、認証情報付加回数管理手段107の証明書を発行回数を1加算し、領域構成バージョン602と、A局の事業者領域容量603と、B局の事業者領域容量604と、A局認証情報605と、B局認証情報606と、領域管理サーバの署名607と、A局を示す利用者識別608と、A局から受信した利用者の証明書609とを含む領域管理サーバの証明書600を作成し、領域管理サーバ1の秘密鍵で暗号化(S323)し、放送局4に送信する(S324)。

【0129】

A局は、領域管理サーバ1の証明書とBMLスクリプトからBMLコンテンツを作成し、記録媒体2を使用している受信機3に送信する(S325)。

【0130】

受信機3はBMLコンテンツを受信し、BMLスクリプトに従い、購入終了画面をBMLブラウザで表示し(S326)、利用命令に従い、BMLスクリプトと証明書を記録媒体2に送信する。

【0131】

記録媒体2では、領域管理サーバ認証手段211が、領域管理サーバ認証情報管理領域202rから領域管理サーバの秘密鍵を取り出し、領域管理サーバ1の証明書を復号し、領域管理サーバ1の署名を確認し、確認できた場合は、領域構成バージョンを領域構成バージョン比較手段212に送信し(S327)、確認できなかった場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0132】

領域構成バージョン比較手段212では、領域構成バージョン管理領域201vから領域構成バージョンを取得し、領域管理サーバ1の証明書に記述されている領域構成バージョンと比較し、一致している場合は、証明書を利用者認証手段213に送信し(S328)、不一致の場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0133】

利用者認証手段213では、A局認証情報管理領域202aからA局の秘密鍵を取り出し、A局の証明書を復号し、A局の署名を確認し、確認できた場合は、BMLスクリプトと証明書を利用命令改竄検出手段214に送信する(S329)。

【0134】

利用命令改竄検出手段214では、BMLスクリプトのハッシュ値を計算し、領域管理サーバ1の証明書に含まれているBMLスクリプトのハッシュ値と比較し(S330)、一致している場合は、利用命令に従って、A局の事業者領域203aに購入した商品の購入履歴を記録し(S331)、不一致の場合は、異常終了を受信機3に通知し(S341)、受信機3で異常終了画面を表示する(S342)。

【0135】

(記録媒体の持ち回り)

記録媒体2の所有者は、記録媒体2を受信機3から抜き出して他の受信機3に挿入することで、記録媒体2を利用するサービスについては、記録媒体2の所有者の家庭にある受信機3と同様にサービスを受信することができる。図15は、他の受信機3を用いてサービスを利用する際の処理を示すフローチャートである。

【0136】

記録媒体2の所有者が記録媒体2をホテル等外出先の受信機3に挿入すると(S401)、受信機3から記録媒体2へ起動命令が送信され、記録媒体2では起動処理が開始される(S402)。

【0137】

記録媒体2の起動処理では、領域構成バージョン比較手段212で領域構成バージョン管

10

20

30

40

50

理領域 201 v から領域構成バージョンを取得 (S403) し、例えば “1.1” という初期化後の値であるため初期化済みであると判断 (S404) し、受信機 3 に個人認証をするための認証情報要求を通知する (S405)。

【0138】

初期化済みでない場合は、領域構成が必要であると判断し、受信機 3 に領域構成要求を通知し (S340)、図 8 の S106 以降の処理を行う。

【0139】

受信機 3 はパスワード入力画面を表示する (S406)。

【0140】

記録媒体 2 の所有者がパスワードを入力すると、受信機 3 は記録媒体 2 にパスワードを送信する (S407)。

【0141】

記録媒体 2 では、個人認証手段 217 において、受信機 3 から受信したパスワードと個人認証情報管理領域 202 k に記録されている認証情報と比較する (S408)。

【0142】

記録媒体 2 は、パスワードが一致していれば、起動完了を受信機 3 に通知する (S409)。

【0143】

記録媒体 2 の起動完了後 (S411) は利用命令による領域管理サーバの専用領域 203 の利用が可能となり、記録媒体 2 の所有者は家庭内の受信機 3 と同様に外出先の受信機でもサービスを受信することができる。

【0144】

なお、汎用領域 204 に記録された情報は、個人認証とは無関係に利用が可能であるため、汎用領域 204 に記録された楽曲データなどは、個人認証機能のない受信機でも利用可能である。

【0145】

なお、本実施の形態では、パスワードによる個人認証を行っているが、領域管理サーバ 1 と記録媒体 2 との通信に SSL などの公開鍵暗号を用いて認証を行う場合であれば、記録媒体 2 の出荷時に記録されている図 1 には示さない証明機関が発行した証明書を記録媒体 2 の所有者からの通知により、証明機関が CRL (Client Revoke List) に加えることで、領域管理サーバ 1 が SSL などの記録媒体 2 からの認証通信を拒否する方法で、記録媒体 2 を無効化してもよい。

【0146】

(放送局の記録媒体利用への課金)

記録媒体 2 は、書き込み回数アップロード日時 201 u に記録された日時に、領域管理サーバ 1 へ書き込み回数をアップロードする。

【0147】

記録媒体 2 は、A 局の事業者領域書き込み回数 201 a k と B 局の事業者領域書き込み回数 201 b k から書き込み回数を読み込み、領域管理サーバ 1 に通知する。

【0148】

記録媒体 2 と領域管理サーバ 1 との通信は、SSL などのセキュアな通信路で行う。

【0149】

領域管理サーバ 1 は、記録媒体 2 からアップロードされた書き込み回数を書き込み回数管理手段 104 に記録する。

【0150】

領域管理サーバ 1 は、定期的、例えば 1 ヶ月毎、に記録媒体 2 を利用している放送局 4 に記録媒体の利用に対する課金を行う。

【0151】

例えば、領域管理サーバ 1 が設定した記録媒体 2 の月額利用料金として、記録媒体数管理手段 105 で管理されている記録媒体 2 の登録数に対して、(1) 領域構成情報管理手段

10

20

30

40

50

101で管理している事業者領域容量1MB毎に10円として加算、(2)1ヶ月の容量変更1回毎に100円として加算する。また、(3)認証情報付加回数管理手段107で管理されている1ヶ月の認証情報付加1回毎に20円として加算する。また、書き込み回数管理手段104で管理している全記録媒体2の1ヶ月の書き込み1回毎に30円として加算する。

【0152】

このような月額利用料金において、例えば、領域管理サーバ1の領域構成情報管理手段101が図7に、認証情報付加回数管理手段107が図17に、書き込み回数管理手段104が図18に示す状態であり、記録媒体数管理手段105で管理されている記録媒体2の登録数が“1000枚”である場合のA局の利用料金の算出例を示す。

10

【0153】

領域構成情報管理手段101からは、A局の記録媒体2の事業者領域容量が“5MB”で、1ヶ月の容量変更回数が“1回”であることが分かる。また、認証情報付加回数管理手段107からは、認証情報付加手段103でA局の証明書を発行した回数が“30回”であることが分かる。さらに、書き込み回数管理手段104からは、全記録媒体2から受信した記録媒体2のA局の事業者領域203aへの書き込み回数の合計が“10000回”であることが分かる。また、記録媒体数管理手段105からは、記録媒体2の登録数が“1000枚”であることが分かるため、

(1)事業者領域容量の料金は、

$$10 \text{ (円/MB)} \times 5 \text{ (MB)} \times 1000 \text{ (枚)} = 50,000 \text{ (円)}$$

20

(2)容量変更の料金は、

$$100 \text{ (円/回)} \times 1 \text{ (回)} \times 1000 \text{ (枚)} = 100,000 \text{ (円)}$$

(3)認証情報付加の料金は、

$$20 \text{ (円/回)} \times 30 \text{ (回)} = 600 \text{ (円)}$$

(4)書き込みの料金は、

$$30 \text{ (円/回)} \times 10000 \text{ (回)} = 300,000 \text{ (円)}$$

として算出される総計450,600円をA局へ課金する。

【0154】

放送局4は、利用料支払手段405で決済処理を行い、領域管理サーバ1に記録媒体2の利用料金を支払う。

30

【0155】

このようにして利用状況に応じて放送局4から徴収した記録媒体2の利用料金の上記(1)～(4)をすべて、または、上記(1)～(4)のいずれかのみが領域管理サーバ1から記録媒体2のメーカーに支払われる。

【0156】

メーカーは領域管理サーバ1から受領する記録媒体2の利用料金を販売価格の一部に充当することを見込んで、記録媒体2を安価に提供することが可能になる。

【0157】

なお、本実施の形態では、記録媒体2の領域管理サーバの専用領域203を利用する利用命令として、情報を記録する利用命令と、領域更新するための利用命令と、情報を読み出す利用命令とを説明したが、例えば、領域管理サーバの専用領域203の破断を修正する命令など、領域管理サーバの専用領域203の利用に関係する利用命令があってもよい。

40

【0158】

なお、本実施の形態では、データ放送による通信販売の例を説明したが、領域管理サーバの専用領域203へのCM視聴ログまたは各種ポイントの記録、および共用領域203kに記録されたユーザ嗜好情報に基づくEPGの記録など、認証された利用者が領域管理サーバの専用領域203を利用する他のサービスがあってもよい。

【0159】

なお、本実施の形態では、放送局を記録媒体2の利用者としたが、領域管理サーバ1への利用者登録に制限はない。

50

【0160】

なお、本実施の形態では、主にデータ放送で利用命令を配信しているが、通信で配信してもよい。

【0161】

なお、本実施の形態では、BMLの放送用拡張関数として利用命令を配信しているが、BML以外の記述言語を用いてもよい。

【0162】

【発明の効果】

本発明によれば、受信機に実装された永続記憶装置の代わりに、受信機から着脱可能で情報の安全な記録が可能な記録媒体に、データ放送で情報の記録を行うため、放送局が、書き換え寿命を考慮して利用を自主規制する必要がなく、記録媒体の所有者のプライバシー情報やポイント情報などを安全に記録することが可能となる。

【0163】

また、利用状況に応じて放送局に記録媒体のコストを負担させるため記録媒体を安価に提供することが可能となる。

【図面の簡単な説明】

【図1】本実施の形態に係る情報記録配信システムの全体の概略構成を示す図

【図2】本実施の形態に係る領域管理サーバ1の構成を示す機能ブロック図

【図3】本実施の形態に係る記録媒体2の概略構成を示す図

【図4】本実施の形態に係る放送局4の構成を示す機能ブロック図

【図5】本実施の形態に係る初期化前の記録媒体2の記録領域の構成を示す図

【図6】本実施の形態に係る領域管理サーバの証明書600の構成を示す図

【図7】本実施の形態に係る領域構成情報管理手段101で管理するテーブルの一例を示す図

【図8】本実施の形態に係る記録媒体2の初期化処理を示すフローチャート

【図9】本実施の形態に係る利用者の証明書609を含む領域管理サーバの証明書600の構成を示す図

【図10】本実施の形態に係る記録媒体2の領域構成を変更する処理を示すフローチャート

【図11】本実施の形態に係る記録媒体の利用処理を示すフローチャート

【図12】本実施の形態に係る記録媒体の利用処理を示すフローチャート

【図13】本実施の形態に係る記録媒体の利用処理を示すフローチャート

【図14】本実施の形態に係る購入画面を示す図

【図15】本発明の実施の形態に係る他の受信機を用いてサービスを利用する処理を示すフローチャート

【図16】本発明の実施の形態に係る記録媒体2の記録領域の一般的なデータ構造を示す図

【図17】本発明の実施の形態に係る認証情報付加回数管理手段107で管理するデータの一例を示す図

【図18】本発明の実施の形態に係る書き込み回数管理手段104で管理するデータの一例を示す図

【符号の説明】

1 領域管理サーバ

2 記録媒体

3 受信機

4 放送局

5 配信サーバ

101 領域構成情報管理手段

102 領域構成変更指示手段

103 認証情報付加手段

10

20

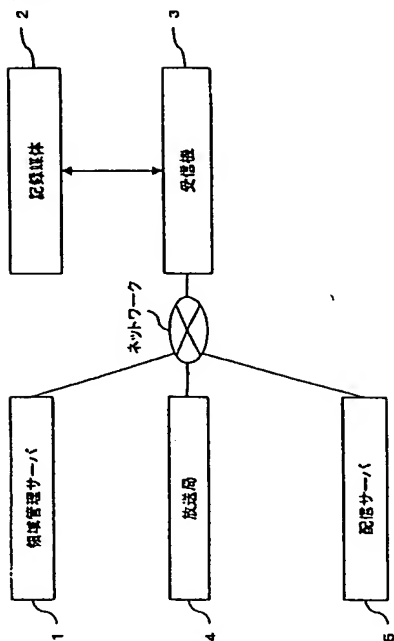
30

40

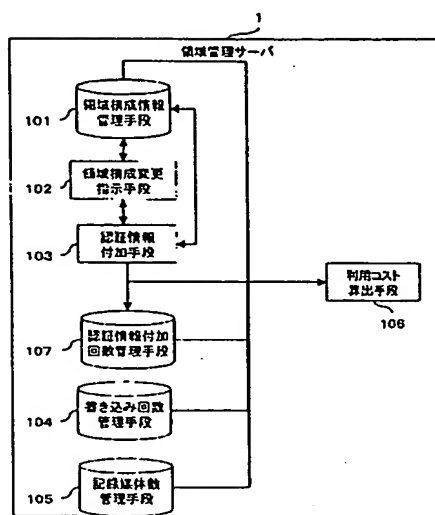
50

104	書き込み回数管理手段	
105	記録媒体数管理手段	
106	利用コスト算出手段	
107	認証情報付加回数管理手段	
201	領域管理情報領域	
201v	領域構成バージョン管理領域	
201a	A局の事業者領域容量	
201b	B局の事業者領域容量	
201u	書き込み回数アップロード日時	
201ak	A局の事業者領域書き込み回数	10
201bk	B局の事業者領域書き込み回数	
202	認証情報管理領域	
202r	領域管理サーバ認証情報管理領域	
202k	個人認証情報管理領域	
202a	A局認証情報管理領域	
202b	B局認証情報管理領域	
203	領域管理サーバの専用領域	
203a	A局の事業者領域	
203b	B局の事業者領域	
203h	ヒープ領域	20
203k	共用領域	
204	汎用領域	
211	領域管理サーバ認証手段	
212	領域構成バージョン比較手段	
213	利用者認証手段	
214	利用命令改竄検出手段	
215	領域構成更新手段	
216	領域構成情報要求手段	
217	個人認証手段	
218	記録媒体識別	30
401	データ放送制作手段	
402	認証情報作成手段	
403	認証情報要求手段	
404	容量変更指示手段	
405	利用料支払手段	
600	領域管理サーバの証明書	
601	スクリプトのハッシュ	
602	領域構成バージョン	
603	A局の事業者領域容量	
604	B局の事業者領域容量	40
605	A局の認証情報	
606	B局の認証情報	
607	領域管理サーバの署名	
608	利用者識別	
609	利用者の証明書	
610	利用者の署名	

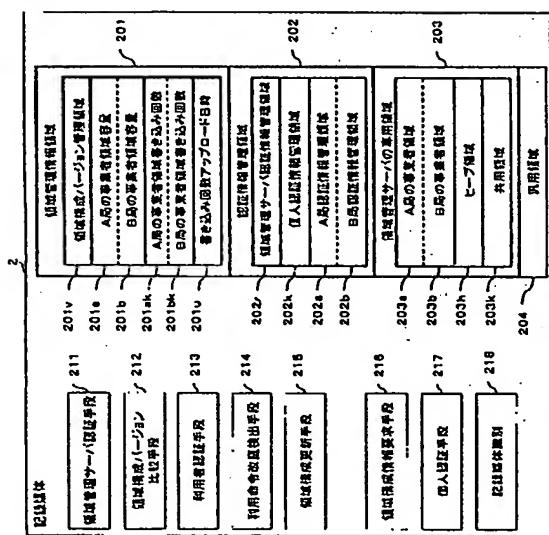
【 図 1 】



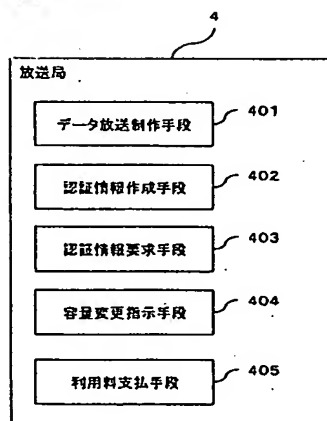
【图 2】



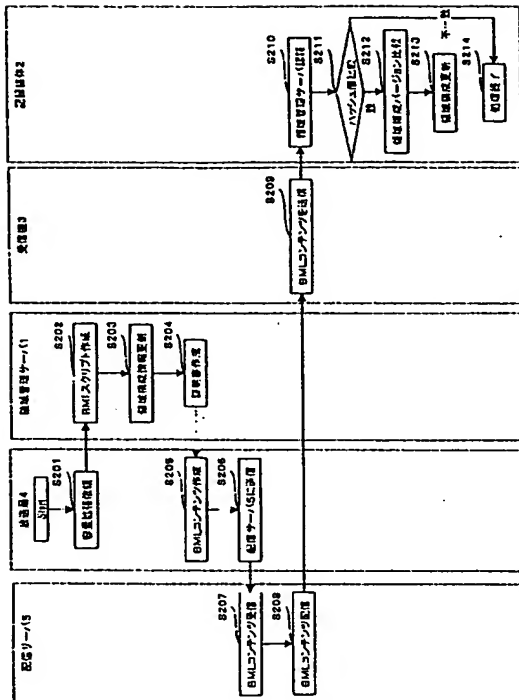
【 図 3 】



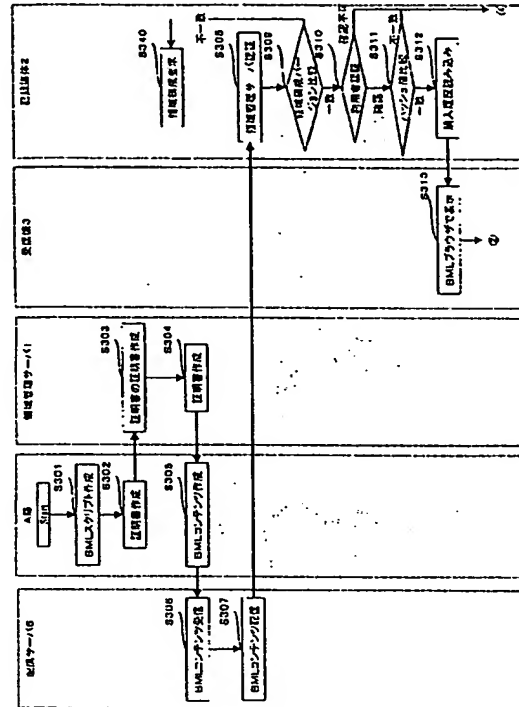
【圖 4】



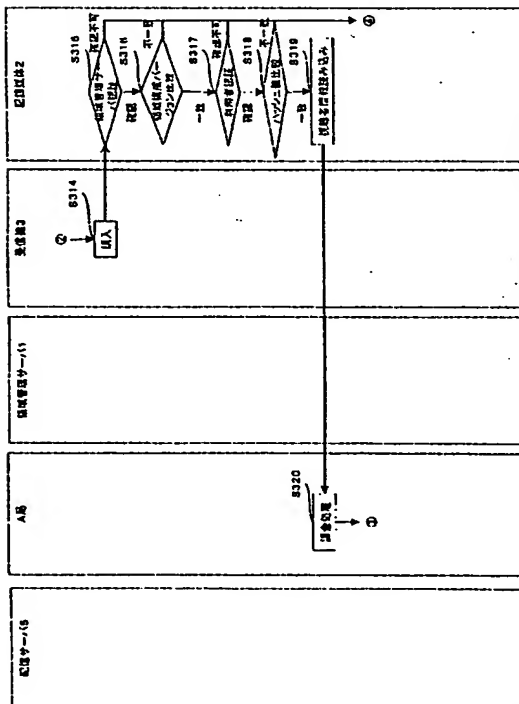
【 10 】



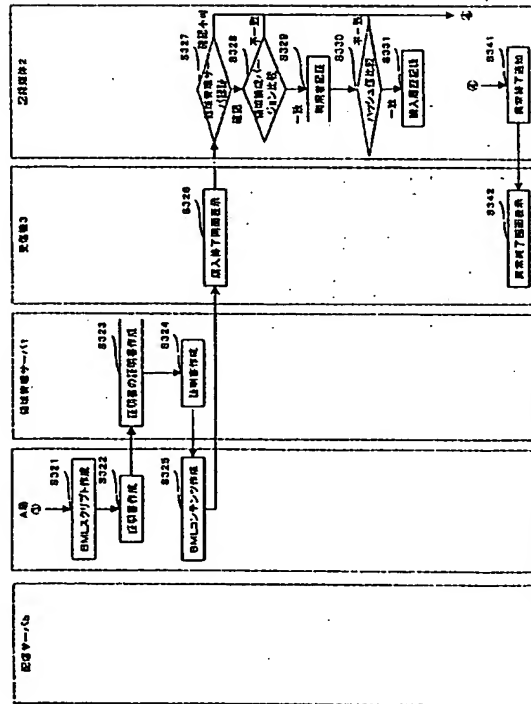
【 11 】



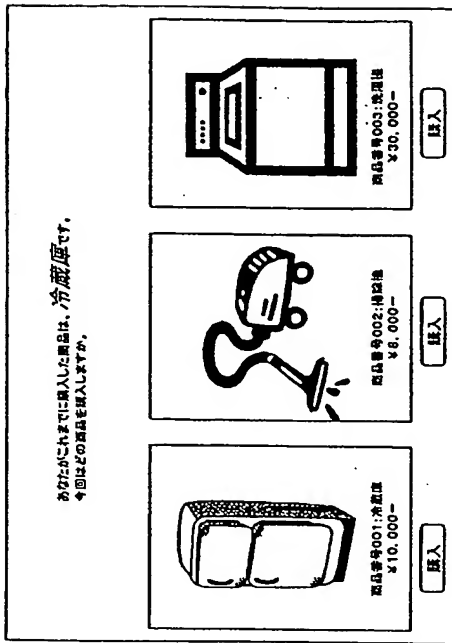
【 12 】



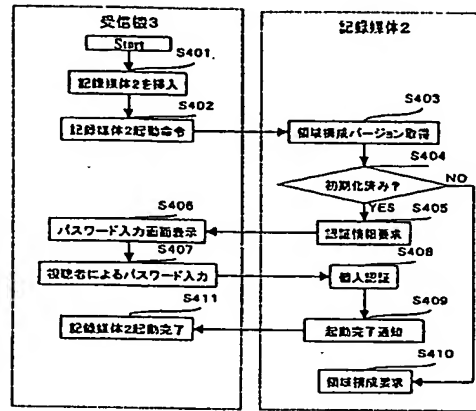
【 13 】



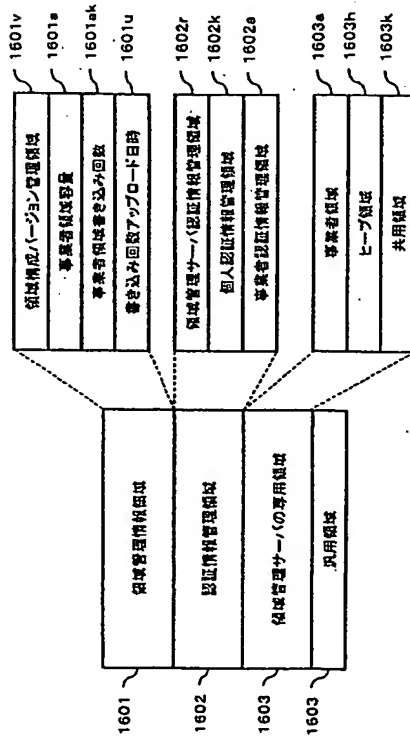
【図14】



【図15】



【図16】



【図17】

事業者	認証情報付加回数
A局	30回
B局	2回

【図18】

事業者	書き込み回数
A局	10000回
B局	200回

フロントページの続き

(51) Int. Cl.⁷

F I

テーマコード (参考)

H 0 4 N 7/16

H 0 4 N 7/16

A

H 0 4 L 9/00 6 7 5 B

(72) 発明者 村上 弘規

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72) 発明者 井上 光啓

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

(72) 発明者 大森 基司

大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

Fターム (参考) 5B017 AA07 BA01 BA05 CA14

5C052 AB04 DD02 DD04

5C064 BA07 BB05 BC12 BC20 BC25 BD09

5J104 AA08 LA03 PA05